AMENDMENTS TO THE CLAIMS

Please amend the claims by replacing the original claims with the following listing of claims.

LISTING OF THE CLAIMS:

1. (Previously presented) A method for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising: providing a hash code table of a client said hash code table being provided for storing a plurality of files; providing a client state code of a client; comparing said client state code to said hash code table, and generating an alert mechanism when a deviation threshold is reached based on a deviation between said hash code table values for said client and said client state code; wherein said secure hash code table includes the hash codes for files on computers within the network that are to be secured;

the method further including:

transmitting across a network from clients located in the network a client state code;

providing at least one server within the network assigned to recognize said client state code transmission,

wherein said server maintains a baseline for said client, and

wherein said baseline comprises said hash code table of a said client.

2. (Original) A method as in claim 1 wherein the step of providing a hash code table of a network device further comprises providing a secure hash code table.

3. (Original) A method as in claim 2 wherein the step of providing a secure hash code table further comprises generating a secure hash code table.

4. (Original) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one compiled client hash value.

5. (Previously presented) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one compiled client hash value, wherein said compiled client hash value is generated by: providing a secure system state data file; grouping said secure system data file into one or more groups; and, extracting the modal hash value from any of said groups.

6. (Original) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one exemplary system.

7. (Original) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one baseline secure value.

8. (Original) A method as in claim 1 further comprising the step of reporting the results of said comparison.

9. (Original) A method as in claim 1 further comprising the step of logging the results of said comparison.

10. (Original) A method as in claim 1 further comprising the step of securing a client in lock down mode.

11. (Original) A method as in claim 1 further comprising the step of initiating a client status mechanism.

12. (Original) A method as in claim 1 further comprising the step of initiating an Auto Restore component.

13. (Original) A method as in claim 1 wherein the step of providing a client state code further comprises generating a client state code.

14. (Original) A method as in claim 3 wherein the step of generating a client state code further comprises generating a client state code using at least one compiled client hash value.

15. (Previously presented) A computer storage component including software containing the hash code table generated by any of the methods of claims 4 through 7.

16. (Previously presented) An article of manufacture comprising a computer storage media that implements code for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising a client state code.

17. (Previously presented) An article of manufacture comprising a computer storage media that implements code for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising a hash code table.

18. (Previously presented) An apparatus for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising: means for providing a hash code table of a client said hash code table being provided for storing a plurality of files wherein said hash code table includes the hash codes for files on computers within the network that are to be secured; means for providing a client state code of a client; means for comparing said client state code to said hash code table; and means for generating an alert when a deviation threshold is reached based on a deviation

between said hash code table values for said client and said client state code.

19. (Previously presented) An apparatus for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising: means for providing a hash code table of a client said hash code table being provided for storing a plurality of files wherein said hash code table includes the hash codes for files on computers within the network that are to be secured; means for providing a client state code of a client; and, means for comparing said client state code to said hash code table, wherein said hash code table is operable for one or more client platforms.

20. (Original) An apparatus as in claim 19 further comprising means for generating a secure hash code table.

21. (Original) An apparatus as in claim 19 further comprising means for reporting the results of said comparison.

22. (Original) An apparatus as in claim 19 further comprising means for logging the results of said comparison.

23. (Original) An apparatus as in claim 19 further comprising a client status mechanism means.

24. (Original) An apparatus as in claim 19 further comprising an Auto Restore component means.

25. (Previously presented) A method for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising: providing a hash code table of a client; providing a client state code of a client; comparing said client state code to said hash code table, wherein said hash code table is operable for one or more client platforms.

26. (Previously presented) The method of claim 25, wherein providing a hash code table includes gathering baseline values to define modal values and generating said hash code table using said defined modal values, wherein each of said clients uses the same or different operating platform as another of said client, and wherein regardless of the operating platform used by a said client, said client state code is compared to said generated hash code table.

27. (Previously presented) The method of claim 25, wherein providing a hash code table further includes transmitting a secure system state data file from a said client to a server, and constructing said hash code table from network clients based on one or more compiled client hash values, the method including grouping secure system state data files into client groups.

28. (Previously presented) The method of claim 1, wherein said clients within said network are identical clients, and wherein said client state codes of the said identical clients are identical.

29. (Previously presented) The method of claim 1, wherein said clients within said network have one or more files present thereon which are common to one or more clients on said network, said files,

wherein said hash code table includes file names and hash codes which are concatenated and stored in said table.

30. (New) The method of claim 1, wherein said method involves initiating a client process from a computer, and wherein providing a hash code table of a client comprises providing a hash code table for the computer from which the client process was initiated.

31. (New) The method of claim 1, wherein the client state code is transmitted along with authentication.